

# A short note on reduced residues

By PASCAL STUMPF

## Abstract

We solve a problem due to Recamán about the lower bound behavior of the maximum possible length among all arithmetic progressions in the least reduced residue system modulo  $n$ , as  $n \rightarrow \infty$ .

## 1. Introduction

For any positive integer  $n > 1$ , let  $\mathcal{A}(n) = \{a \in \mathbb{Z}^+ : a < n, (a, n) = 1\}$  be the (nonempty) set of all smaller positive integers relatively prime to  $n$ , or in other words the least reduced residue system modulo  $n$ , and define  $f(n)$  as the maximum possible length among all arithmetic progressions in  $\mathcal{A}(n)$ . In a letter from 1995 [1] Bernardo Recamán asked if  $f(n)$  tends to infinity with  $n$ , i.e. if for each  $k \in \mathbb{Z}^+$  there exists a constant  $n_k$  such that  $\mathcal{A}(n)$  contains an arithmetic progression of length  $k$  for all  $n \geq n_k$ .

One very nice but deep result coming to mind here is that of Ben Green and Terence Tao [2] telling us about arbitrary long arithmetic progressions in the primes, and in fact it is a promising indicator for a positive answer to our question, since  $\mathcal{A}(n)$  contains all primes less than  $n$  except its prime factors. However, it turns out that we can prove the truth of our conjecture by using only elementary methods, and in what follows we like to present one possible (hopefully cute) solution. But before we start, let us consider a few examples to become even more familiar with our notations and the problem itself:

$n$	$\mathcal{A}(n)$	$f(n)$	$n$	$\mathcal{A}(n)$	$f(n)$
2	$\{1\}$	1	12	$\{1, 5, 7, 11\}$	2
3	$\{1, 2\}$	2	13	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$	12
4	$\{1, 3\}$	2	14	$\{1, 3, 5, 9, 11, 13\}$	4
5	$\{1, 2, 3, 4\}$	4	15	$\{1, 2, 4, 7, 8, 11, 13, 14\}$	3
6	$\{1, 5\}$	2	16	$\{1, 3, 5, 7, 9, 11, 13, 15\}$	8
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

## 2. Ideas and Proof

First, let us suppose  $n$  is prime: then all of the numbers  $1, \dots, n-1$  are relatively prime to  $n$  and form an arithmetic progression of length  $n-1$  with common difference 1, which means  $f(n) = n-1$ . In the more general case of a prime power  $n = p^r$ , where  $p$  is prime and  $r \in \mathbb{Z}^+$ , we similarly still have  $\{1, \dots, p-1\} \subset \mathcal{A}(n)$  and thus  $f(n) \geq p-1$ , but if  $r \geq 2$  we can also look at the numbers  $1 + m \cdot p$  for  $0 \leq m < p^{r-1}$ , all of them lying in  $\mathcal{A}(n)$  since none of them being divisible by  $p$ , and forming an arithmetic progression of length  $p^{r-1}$  with common difference  $p$ , giving us even  $f(n) \geq p^{r-1} = n/p$  here.

Now let us consider squarefree numbers  $n = p_1 p_2 \dots p_d$ , where  $d \geq 2$  and  $2 \leq p_1 < p_2 < \dots < p_d$  (odd) are prime. Like before, a good idea seems to be looking at numbers of the form  $1 + m \cdot q$ , this time choosing  $q = p_1 p_2 \dots p_{d-1}$  and  $0 \leq m < p_d$ , which ensures us that

$$a_m = 1 + m \cdot q \leq 1 + (p_d - 1) \cdot q = 1 + n - q \leq 1 + n - 2 < n$$

is not divisible by any of the primes  $p_1, p_2, \dots, p_{d-1}$ , although we are not sure about non-divisibility by  $p_d$  yet. However, together  $a_0, a_1, \dots, a_{p_d-1}$  represent a complete residue system modulo  $p_d$ , because if  $a_x \equiv a_y \pmod{p_d}$  for some  $0 \leq x < y < p_d$  (\*), then  $0 \equiv a_y - a_x = (y - x) \cdot q \pmod{p_d}$  and  $(q, p_d) = 1$  would imply  $(y - x) \equiv 0 \pmod{p_d} \Leftrightarrow x \equiv y \pmod{p_d}$  in contradiction to (\*). In particular only one member of  $a_0, a_1, \dots, a_{p_d-1}$  is divisible by  $p_d$ , say  $a_m$ , and so by the box principle we get that  $a_0, \dots, a_{m-1}$  or  $a_{m+1}, \dots, a_{p_d-1}$  is an arithmetic progression of length at least  $(p_d - 1)/2$  with common difference  $q$  completely contained in  $\mathcal{A}(n)$ , which delivers  $f(n) \geq (p_d - 1)/2$ .

Finally, let us introduce exponents  $r_1, r_2, \dots, r_d \in \mathbb{Z}^+$  such that we can cover all remaining numbers  $n = p_1^{r_1} p_2^{r_2} \dots p_d^{r_d}$ , where  $r_1 + r_2 + \dots + r_d > d$ . Because  $n$  has the same prime factors as  $p_1 p_2 \dots p_d$ , we get  $\mathcal{A}(p_1 p_2 \dots p_d) \subset \{a + m \cdot p_1 p_2 \dots p_d : a \in \mathcal{A}(p_1 p_2 \dots p_d), 0 \leq m < p_1^{r_1-1} p_2^{r_2-1} \dots p_d^{r_d-1}\} = \mathcal{A}(n)$  by observing  $(a, n) = 1 \Leftrightarrow (a, p_1 p_2 \dots p_d) = 1$  running over all integers  $a$ , and hence  $f(n) \geq f(p_1 p_2 \dots p_d) \geq (p_d - 1)/2$ . On the other hand, we might again do better by looking at the numbers  $1 + m \cdot p_1 p_2 \dots p_d$  forming an arithmetic progression of length  $p_1^{r_1-1} p_2^{r_2-1} \dots p_d^{r_d-1}$  with common difference  $p_1 p_2 \dots p_d$ , and both ideas in one lead us to  $f(n) \geq \max\{(p_d - 1)/2, n/(p_1 p_2 \dots p_d)\}$ .

After we obtained lower bounds on  $f(n)$  according to all possible prime factorizations of  $n$ , we are almost ready to prove our main result, but first let us collect them in the following more compact statement:

**LEMMA 2.1.** *For  $n > 1$  we have  $f(n) \geq \max\{(p-1)/2, n/P\}$ , where  $p$  is the largest prime factor of  $n$  and  $P$  is the product of all prime factors of  $n$ .*

LEMMA 2.2. *For each  $k \in \mathbb{Z}^+$  there exists a constant  $n_k$  such that  $\mathcal{A}(n)$  contains an arithmetic progression of length  $k$  for all  $n \geq n_k$ .*

*Proof.* Let  $P_{2k}$  be the product of all primes not exceeding  $2k$  and define  $n_k = k \cdot P_{2k} \geq 1 \cdot 2$ . Moreover, let us fix any  $n \geq n_k$  and (as in Lemma 2.1) denote its largest prime factor by  $p$ . If  $p \geq 2k + 1$ , we immediately arrive at  $(p - 1)/2 \geq ((2k + 1) - 1)/2 = k$ . But then in the other case  $p < 2k + 1$ , we note that all prime factors of  $n$  do not exceed  $2k$ , implying their product  $P$  divides  $P_{2k}$ , and so, in particular,  $n/P \geq n_k/P = k \cdot P_{2k}/P \geq k$ . Combining everything we get  $f(n) \geq \max\{(p - 1)/2, n/P\} \geq k$ , and our claim follows.  $\square$

Captured by Lemma 2.2, we mainly worked on lower bounds so far and almost forgot about searching for possible upper bounds on  $f(n)$ . In order to catch up on them, let us change our point of view and conclude by showing:

LEMMA 2.3. *For  $n > 1$  we have  $f(n) \leq \max\{(p - 1)/1, n/P\}$ , where  $p$  is the largest prime factor of  $n$  and  $P$  is the product of all prime factors of  $n$ .*

*Proof.* Suppose  $a_0, a_1, \dots, a_{s-1}$  is an arithmetic progression contained in  $\mathcal{A}(n)$  with common difference  $q$  and length  $s$ . Now we focus a bit more on  $q$ : If  $q \geq P$ , we can only come up to  $s \leq n/P$ , since otherwise  $s > n/P$  implies  $a_{s-1} = a_0 + (s - 1) \cdot q \geq 1 + ((n/P + 1) - 1) \cdot P \geq n + 1$  and our last member would not be in  $\mathcal{A}(n)$  anymore. In the other case, we have  $q < P$ , yielding  $q$  is missing at least one prime factor  $p'$  of the squarefree number  $P$  dividing  $n$ . But then  $(q, p') = 1$  once again, like around (\*), whispers us that, whenever  $s \geq p'$ , the first  $p'$  members  $a_0, a_1, \dots, a_{p'-1}$  do represent a complete residue system modulo  $p'$ , and thereby one of them, being a multiple of  $p'$ , could not ly within  $\mathcal{A}(n)$  anymore, leaving us only  $s \leq p' - 1 \leq p - 1$  left here. Uniting both cases we reach  $f(n) \leq \max\{n/P, p - 1\}$ , as desired.  $\square$

*Acknowledgements.* All my thanks to Miriam (and Christian) for always encouraging me to write things down and making my first paper possible.

## References

- [1] RICHARD GUY, *Unsolved Problems in Number Theory*, Springer (2004), 146–147.
- [2] BEN GREEN and TERENCE TAO, The primes contain arbitrarily long arithmetic progressions, *Annals of Mathematics* **167** (2008), 481–547.

*e-mail:* littlefriend@mathlino.org